Hitachi Vantara

Solution Profile

Achieve Cyber Resilience With a Risk-Optimized Data Foundation

Be Audit-Ready

Strengthen stakeholder and regulatory confidence with provable, tested resilience and built-in audit trails.

Cut MTTR at Scale

Reduce Mean Time to Recovery to hours with automated, guaranteed clean recovery points at petabyte scale[1].

Reduce Complexity

Cut tool and skill gaps with a standards-aligned, risk-tiered architecture that simplifies resilience operations.

Turn cyberattacks into predictable continuity with standards-aligned data-layer resilience tailored to critical operations and compliance obligations.

Today's cyber landscape makes downtime and data corruption a board-level business risk, not a back-office IT issue. Organizations face escalating ransomware, fragmented hybrid estates and rising regulatory scrutiny that turn every cyberattack into a business, financial and compliance event. They need a data-first, risk-optimized cyber resilience solution that can contain attacks, recover clean data and restore critical services at scale with confidence.

The Hitachi solution organizes data into business-criticality- and regulation-aligned resilience zones with tamper-proof copies, continuous anomaly detection and isolated recovery paths. It then orchestrates automated, guaranteed clean recovery points to bring priority services online in hours instead of days.

This integrated approach aligns security, infrastructure and operations around a unified, standards-based architecture and expert services that reduce tool and skill gaps while improving auditability. As a result, you can shrink the blast radius of attacks, lower regulatory and financial risk, and demonstrate predictable business continuity at petabyte scale to boards, regulators, customers and insurers.

Gain Operational Confidence

Run on a data foundation Fortune 100® leaders trust, backed by resilience guarantees.

Rely on Clean Recovery

Limit data loss to minutes with 2X faster, AI-validated clean snapshot-based recovery[2].

Simplify Business Continuity

Align data resilience to criticality and regulation to recover mission-critical services in hours.

Maximize Investments

Enhance your existing infrastructure and security stack with platform-agnostic flexibility and built-in integrations.

Achieve Cyber Resilience With a Risk-Optimized Data Foundation

Today's Challenge: Resilience Amid Uncertainty, Regulation and Complexity

Ransomware attacks are now AI-driven, automated and financially motivated. They target data as the fastest route to operational disruption and extortion — making data resilience the foundation of true cyber resilience.

Hybrid data estates across data centers, clouds, SaaS and third parties have expanded the attack surface beyond what traditional prevention and backup tools can reliably protect. At the same time, organizations must meet resilience-focused mandates, such as the European Union's Digital Operational Resilience Act (DORA), along with similar rules across Europe, North America, Asia Pacific and the Middle East. These requirements demand not just security controls but also demonstrably recoverable, validated data, with fines that can reach up to 10% of annual revenue[3].

Boards, customers, insurers and auditors are no longer asking "Are you protected?" but "Can you prove critical services will remain available during and after an attack?"

Operational complexity magnifies this risk. Security, infrastructure and application teams often work in silos with overlapping tools and no single owner for recovery SLAs.

During an incident, fragmented prevention and backup tooling, cross-functional handoffs, and skills shortages slow decisions when minutes matter. This drives longer downtime, greater data loss and uncertainty about whether recovered data is truly clean.

Modern cyber, regulatory and market forces make strengthening data resilience a near-term business imperative, not an IT optimization.

A Unified, Risk-Optimized Data Resilience Solution

Hitachi Vantara delivers a unified data resilience solution that shrinks the blast radius of cyberattacks and keeps critical systems running and compliant when attacks succeed. It focuses on the data itself, using the NIST Cybersecurity Framework 2.0 (NIST CSF 2.0) to govern how data is protected, how fast you can recover it, and how you prove it is clean.

- **Before an Attack:** Data is organized into "data resilience zones" based on business risk and regulatory needs. Mission-critical data sits in zones engineered for downtime measured in hours and data loss measured in minutes, while other important data is placed in zones optimized for efficiency and long-term retention. Each zone uses hardened, immutable data copies, integrity checks and clear recovery paths that can be tested in isolated environments, so you know which systems come back first, and from where, with proven recovery.
- **During an Attack:** The solution continuously analyzes production snapshots and backups in each zone to spot indicators of compromise early and identify clean recovery points. Immutable copies cannot be changed by ransomware, which means you have trusted recovery points, even while an incident is still in progress.
- **After an Attack:** Automated recovery orchestration uses those validated clean points to spin up isolated recovery environments and perform initial malware eradication as a fast start for incident response data cleansing. Then, it enables administrators to promote the fully recovered environment back into production, zone by zone, at petabyte scale.

> *"...we can now recover our production systems around **80% faster**."*
>
> **Darren Chapman**,
> Infrastructure Development Manager,
> University of Kent

Use Cases

Cyber Risk Mitigation: Reduce Exposure and Simplify Oversight

Mitigate cyber and regulatory risk with the Hitachi hybrid cloud platform. This unified data and control plane for structured and unstructured workloads delivers NIST CSF 2.0-aligned data resilience zones, policy-driven controls and immutable data copies. Hitachi adds business continuity planning services and risk-based data classification to establish or scale a minimum viable company model. This approach allows you to continuously govern critical data, limit incident impact and demonstrate a stronger, evidence-backed compliance posture.

Cyber Recovery: Accelerate Predictable, Clean Recovery at Scale

- **Mission-Critical Cyber Recovery: Near-Zero Downtime and Data Loss**
  Recover your most critical services from attacks with a guaranteed clean recovery point delivered through the Hitachi hybrid cloud data platform and near-production immutable snapshots. The platform runs an automated cyber recovery architecture: local snapshot recovery points, zero-day integrity scanning and isolated restore-from-snapshot with built-in malware eradication to accelerate data cleansing. It delivers near-zero RTO/RPO for mission-critical workloads, with audit trails and isolated testing that prove continuity at scale.

- **Business-Critical Cyber Recovery: Efficient, Long-Term Retention**
  Protect and recover important but less time-sensitive services with a data-resilient architecture built on immutable backup recovery points and integrity scanned copies. Tiered business-critical data resilience zones are optimized for long-term, cost-efficient retention. They enable predictable restore-from-backup, reduced data loss and audit-ready recovery for large volumes of structured and unstructured data — without overengineering mission-critical SLAs.

Why Hitachi for Cyber Resilience?

Hitachi helps you contain the cyberattack blast radius and recover cleaner in hours, with less data loss at petabyte scale. For regulated, always-on organizations, the unified data resilience solution is backed by guarantees for data availability and clean recovery points and offers flexible self-managed, managed and pay-as-you-use options. By structuring data into risk-based resilience zones with tamper-proof data copies, automated clean recovery and built-in audit trails, organizations can reduce operational disruption, regulatory exposure and complexity.

- **Predictable:** 100% clean cyber recovery point guarantee
- **Proven:** 86% of global Fortune 100 customers
- **Painless:** Up to 79% audit overhead reduction
- **Economical:** Up to 20% TCO reduction versus point solutions

Ready to learn more?
Contact a Hitachi cyber and data resilience expert.

Connect Now →

About Hitachi Vantara

Hitachi Vantara is transforming the way data fuels innovation. A wholly owned subsidiary of Hitachi, Ltd., we're the data foundation the world's leading innovators rely on. Through data storage, infrastructure systems, cloud management and digital expertise, we build the foundation for sustainable business growth.

[1] Subject to the Hitachi Vantara Cyber Resilience Guarantee terms and conditions; please contact your Hitachi Vantara representative for details.

[2] Hitachi lab tests show that Hitachi Thin Image Advanced safe snap snapshots are recoverable in under 30 seconds per snapshot for snapshots taken of 16 TiB or less volumes stored on Hitachi Virtual Storage Platform One Block (VSP One Block).

[3] Source: DLA Piper, DORA Penalty Regimes: Overview of Divergence in Administrative Penalties under DORA, 2025.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
hitachivantara.com | community.hitachivantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
hitachivantara.com/contact

HV-BTD-SP-Achieve-Cyber-Resilience-3Apr26-A